

What is claimed is:

1. An encrypting apparatus, comprising:
 circuit means, having at least one programmable
 logic device, for forming an encrypting circuit with
 the programmable logic device corresponding to given
 encrypting specifications; and

changing means for reading change data for
 changing the encrypting specifications and
 automatically changing the encrypting circuit
 corresponding to the change data.

2. The encrypting apparatus as set forth in
 claim 1, wherein

said changing means includes configuration means
 for writing a mapping data object that represents the
 structure of the encrypting circuit to the
 programmable logic device, and changes the encrypting
 circuit with an existing mapping data object as the
 change data.

3. The encrypting apparatus as set forth in
 claim 1, wherein

said changing means includes:

compiler means for generating a mapping data

object that represents the structure of the encrypting circuit, by compiling a library written in a hardware description language, and

configuration means for writing the mapping data object to the programmable logic device; and

said changing means reads an existing library as the change data, compiles the existing library, and changes the encrypting circuit.

4. The encrypting apparatus as set forth in claim 1, wherein

said changing means includes:

database means for storing an encrypting algorithm file having a predetermined encrypting algorithm,

compiler means for generating a mapping data object that represents the structure of the encrypting circuit, by compiling a library written in a hardware description language, and

configuration means for writing the mapping data object to the programmable logic device; and

said changing means retrieves a relevant encrypting algorithm file and changes the encrypting circuit with the library in the relevant encrypting algorithm file, corresponding to setup data given as

the change data from the outside.

5. The encrypting apparatus as set forth in claim 1, further comprising:

5 network connecting means for connecting the encrypting apparatus to a communication network, wherein

said changing means reads the change data from the communication network.

10

6. The encrypting apparatus as set forth in claim 5, wherein

said network connecting means receives the encrypted change data from the network, and said
15 changing means changes the encrypting circuit corresponding to the encrypted change data.

7. The encrypting apparatus as set forth in claim 1, wherein

20 said changing means periodically updates the encrypting specifications.

8. The encrypting apparatus as set forth in claim 1, wherein

25 said changing means updates the encrypting

40444330

9. The encrypting apparatus as set forth in claim 1, wherein

10

circuit means, having at least one programmable logic device, for forming a decrypting circuit with the programmable logic device corresponding to given decrypting specifications; and

20

SUB 7
C4

25 said changing means includes configuration means
for writing a mapping data object that represents the
structure of the decrypting circuit to the

programmable logic device, and changes the decrypting circuit with an existing mapping data object as the change data.

5 12. The decrypting apparatus as set forth in claim 10, wherein

 said changing means includes:

 compiler means for generating a mapping data object that represents the structure of the decrypting circuit, by compiling a library written in a hardware description language, and

 configuration means for writing the mapping data object to the programmable logic device; and

10 said changing means reads an existing library as the change data, compiles the existing library, and changes the decrypting circuit.

 13. The decrypting apparatus as set forth in claim 10, wherein

20 said changing means includes:

 database means for storing a decrypting algorithm file having a predetermined decrypting algorithm,

 compiler means for generating a mapping data object that represents the structure of the decrypting circuit, by compiling a library written in a hardware

description language, and

configuration means for writing the mapping data object to the programmable logic device; and

5 said changing means retrieves a relevant decrypting algorithm file and changes the decrypting circuit with the library in the relevant decrypting algorithm file, corresponding to setup data given as the change data from the outside.

10 14. The decrypting apparatus as set forth in claim 10, further comprising:

network connecting means for connecting the decrypting apparatus to a communication network, wherein

15 said changing means reads the change data from the communication network.

15. The decrypting apparatus as set forth in claim 14, wherein

20 said network connecting means receives the decrypted change data from the network, and said changing means changes the decrypting circuit corresponding to the decrypted change data.

25 16. The decrypting apparatus as set forth in

2025 RELEASE UNDER E.O. 14176

claim 10, wherein

said changing means periodically updates the decrypting specifications.

5 17. The decrypting apparatus as set forth in claim 10, wherein

said changing means updates the decrypting specifications corresponding to an external command.

10 18. The decrypting apparatus as set forth in claim 10, wherein

said changing means changes the decrypting specifications corresponding to at least one of a communication path of data to be encrypted, a degree of security thereof, and a process speed required therefor.

19. A signal processing apparatus, comprising:
circuit means, having at least one programmable logic device, for forming a circuit corresponding to given specifications; and

changing means for reading change data for changing the specifications of the circuit, the change data representing one of encrypting specifications or
25 decrypting specifications, and automatically changing

SECRET

Sub-20
a3

the circuit corresponding to the change data.

20. An encryption processing system for use with a communication system for exchanging encrypted data through a communication network, comprising:

encrypting circuit means, having at least one programmable logic device, for forming an encrypting circuit corresponding to given encrypting specifications;

10 encryption changing means for reading encryption change data for changing the encrypting specifications and automatically changing the encrypting circuit corresponding to the encryption change data;

15 decrypting circuit means, having at least one programmable logic device, for forming a decrypting circuit corresponding to given decrypting specifications; and

20 decryption changing means for reading decryption change data for changing the decrypting specifications and automatically changing the decrypting circuit corresponding to the decryption change data.

Sub
DH7

~~21. An encrypting apparatus, comprising:
encrypting means, composed of an unit of which
25 circuit connections for encrypting data can be changed~~

corresponding to an external command, for encrypting data; and

changing means for changing the circuit connections of said encrypting means corresponding to specifications of the encrypting algorithm ^{only} when the specifications are changed.

22. An decrypting apparatus, comprising:

decrypting means, composed of an unit of which circuit connections for decrypting data can be changed corresponding to an external command, for decrypting data; and

changing means for changing the circuit connections of said decrypting means corresponding to specifications of the decrypting algorithm ^{only} when the specifications are changed.

23. An encrypting method, comprising the steps of:

forming an encrypting circuit corresponding to given encrypting specifications with at least one programmable logic device; and

reading change data for changing the encrypting specifications and automatically changing the encrypting circuit corresponding to the change data.

SECRETED

Sub
A4

24. A decrypting method, comprising the steps of:

forming an decrypting circuit corresponding to given decrypting specifications with at least one programmable logic device; and

reading change data for changing the decrypting specifications and automatically changing the decrypting circuit corresponding to the change data.

25. A signal processing method, comprising the steps of:

forming a circuit corresponding to given specifications with at least one programmable logic device; and

reading change data for changing the specifications of the circuit, the specifications representing one of encrypting specifications or decrypting specifications, and automatically changing the circuit corresponding to the change data.

20

SECRET

Add
F8